CPWG Mapping Comparison Matrix

Federal Bridge Certification Authority (FBCA) and the XXXX

For cross certification at a Rudimentary Level of Assurance

Booz | Allen | Hamilton
900 Elkridge Landing Road
Linthicum, MD 21090

Version 2 **4 March 2003**

TABLE OF CONTENTS

1.0 INTRODUCTION

The purposes of this certificate policy comparison, in relation to the comparison study conducted with XXXX [2] and the FBCA CP [3], are:

1) To identify at a rudimentary level the most severe areas of inconsistency and/or similarity between the contents of these two Certificate Policy (CP) documents to cross certify at a Rudimentary Level of Assurance,

2) To identify at a rudimentary level the areas of consistency and/or similarity between the contents of these two Certificate Policy (CP) documents to cross certify at a Rudimentary Level of Assurance, and

3) To recommend appropriate changes, if required, to XXXX [2] that would make it more consistent with the FBCA CP [3];

This document is organized to achieve these purposes in the following sections:

1) **EXECUTIVE SUMMARY**, which provides a high-level overview of the PKIs represented by the Certificate Policies being compared in this analysis as well as an overview of the findings of this mapping comparison,

2) **BRIEF ASSESSMENT**, which provides a brief indication of the degree of similarity of each XXXX as compared to the FBCA CP by indicating the evaluation term used in each main subsection of the CP; and

3) **DETAILED ASSESSMENT**, which presents a detailed breakdown of the requirements in the FBCA CP, Section by Section, and categorizes the degree of similarity of the XXXX requirements to the FBCA CP. Comments to explain the rationale for the degree of similarity are also provided. The topical and organizational framework used as a basis for this comparison is Request for Comments (RFC) 2527, the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [1].

2.0 EXECUTIVE SUMMARY

The Federal Bridge Certification Authority (FBCA) is the unifying element to link autonomous Certification Authorities (CA's) into a systematic overall Public Key Infrastructure (PKI). The FBCA functions as a non-hierarchical hub allowing relying parties to create certificate trust paths from their PKI domains back to the PKI domain of the Certification Authority that issued the certificate, so that the levels of assurance honored by disparate PKI's can be reconciled.

The General Services Administration (GSA), under the auspices of the Federal Public Key Infrastructure Policy Authority (FPKIPA) and the Federal PKI Steering Committee (FPKISC) operates the FBCA. In order to promote interoperability and the appropriate use of certificate policies, the FBCA has issued a minimum set of operational requirements that support trust path creation and verification of digital certificates. The FBCA will issue cross-certificates to other autonomous Principal CA's, and then only when authorized by the FPKIPA. Initially, autonomous CA's that operate in trust domains that meet the requirements established by the FPKIPA will be eligible to cross-certify with the FBCA.

The FBCA is designed to provide a mechanism for entities employing entity-specific PKI's to interoperate efficiently. The FBCA allows entities to create and process trust paths between specific PKI's, so that digital certificates issued by one CA can be honored with an appropriate level of trust [or assurance] by a different CA.

The FBCA acts as a non-hierarchical "hub." A Principal CA receives permission to interoperate with the FBCA under terms and conditions described in the application for cross certification. This system will allow every CA that cross certifies with the FBCA the possibility of interoperating with all participating entities using FBCA-issued cross certificates, in an environment of trust and reliability. This is accomplished through the use of policy mapping, which is how certificates issued in different Entity PKIs meet one another's standards for authentication, integrity of data, non-repudiation, and encryption of data. Policy mappings between the autonomous Principal CA and the FBCA are proposed by the entity and approved by the FPKIPA, and then placed in the certificate issued by the FBCA to the autonomous Principal CA's.

When the Applicant is determining whether to rely on a certificate issued by another Entity or party, it is not required to use the mapping expressed in the FBCA certificates. The Applicant, at its sole discretion, may choose to use a separate mapping for certain transactions or for all transactions.

The XXXX operates a PKI to provide security for its electronic information. The XXXX consists of products and services that provide and manage X.509v3 certificates for public-key cryptography. A XXXX digital certificate identifies the individual named in the certificate requestor/holder, and binds that person to a unique public/private key pair.

Programs that carry out or support XXXX missions may require the type of security services provided by a PKI such as authentication, confidentiality, encryption, non-repudiation, and access control. These services are met with an array of network security components such as web servers, guards, firewalls, routers, and trusted database servers. The operation of these components is supported and complemented by use of public-key cryptography. As a system solution, the components share the burden of the total system security. The use of public key certificates does not add any security services in a poorly designed or implemented system. The reliability of the public-key cryptography portion of the security solution is a direct result of the secure and trustworthy operation of an established PKI, including equipment, facilities, personnel, and procedures.

The XXXX Certificate Policy (CP) follows and complies with the Internet Engineering Task Force (IETF) Request for Comment (RFC) 2527, X.509 PKI CP and Certification Practices Framework. The XXXX defines the primary obligations and operational responsibilities of all XXXX program participants, and defines the creation, management and use of X.509 Version 3 digital certificates. The XXXX defines the applicability of assurance levels for the protection of information based on its value or sensitivity, the risk and the consequences of loss, disclosure or modification.

This Rudimentary Level CP mapping comparison identifies any differences between the FBCA CP and XXXX based on a set of predetermined evaluation terms, defined in the BRIEF ASSESSMENT. The results of this comparison identify the sections that require modification to facilitate policy compatibility and interoperability of the underlying technology and operations.

3.0 BRIEF ASSESSMENT

This section of the report contains the mapping table results, representing a high level view of the mapping comparison between the FBCA CP [3] and the XXXX [2]. This brief assessment in conjunction with the detailed assessment of CP parameters mapped at the Rudimentary Level of Assurance, verify that the XXXX is compliant with the FBCA CP for a cross certification with the FBCA at a Rudimentary Level of Assurance.

The "Brief Assessment" table provides a quick evaluation list to facilitate the quick identification that the XXXX was evaluated against and the "Overall Match" status as compared to the FBCA CP requirement. This table presents a concise indication of the degree of conformity between the XXXX [2] and the FBCA CP [3] at the Rudimentary Level of Assurance. The XXXX Section column is left blank if it is the same as the FBCA Section for the data being analyzed, if a different Section number reference has been inserted, it is the corresponding Section in the XXXX that carries the data that is being compared.

The Brief Assessment table contains four main columns described as follows:

1) **FBCA** – identifies the section numbers for each of the CPs
2) **XXXX Section Topics** – identifies the CP framework section titles corresponding to the section numbers. If there is not a corresponding section in one of the CPs, it is indicated with "N/A" for Not Applicable.
3) **Section Topic** - Title Category
4) **Evaluation Summary –** displays the corresponding evaluation result, which indicates the *lowest* degree of conformity contained within each section.

The following seven evaluation terms and their definitions, listed in order of degree of conformity, were used to assess the **XXXX** CP alignment to the FBCA CP elements:

1) **Exceeds** - The **XXXX** CP policy provides a higher level of assurance/security than the FBCA CP requirement
2) **Equivalent** - The **XXXX** CP policy provides exactly the same assurance/security as the FBCA CP requirement.
3) **Comparable** - The **XXXX** CP contains dissimilar policy contents, but provides a comparable level of assurance to meet the security to the FBCA CP requirement.
4) **Partial** - The **XXXX** CP contains policy that is comparable, but it does not address the entire FBCA CP requirement.
5) **Not Comparable** - The **XXXX** CP contains dissimilar policy contents, which provides a lower level of assurance/security than the FBCA CP requirement.
6) **Missing** - The **XXXX** CP does not contain policy contents that can be compared to the FBCA CP requirement in any way.
7) **N/A** – Not Applicable to **XXXX** CP or required for FBCA cross certification.

RUDIMENTARY LEVEL OF ASSURANCE MAPPING RESULTS

FBCA Section	XXXX Section	Section Topic	Evaluation Summary
	1.0	**INTRODUCTION**	
1.2		Identification	
1.3.4		Applicability	
	2.0	**GENERAL PROVISIONS**	
2.7.1		Frequency of Entity Compliance Audit	
	3.0	**IDENTIFICATION AND AUTHENTICATION**	
3.1.1		Types of Names	
3.1.9		Authentication of Individual Identity	
3.2.1		Certificate Re-Key	
	4.0	**OPERATIONAL REQUIREMENTS**	
4.1.1		Delivery of public key for certificate issuance	
4.4.3.1		CRL issuance requirements	
4.5		Security Audit Procedure	
4.5.2		Frequency of processing data	
4.6.1		Types of events archived	
4.6.2		Retention period for archive	
	5.0	**PHYSICAL, PROCEDURAL AND PERSONELL SECURITY CONTROLS**	
5.2.2		Separation of Roles	
5.2.4		Identification and Authentication for each Role	
	6.0	**TECHNICAL SECURITY CONTROLS**	
6.1.1		FBCA and CA key pair generation	
6.1.8		Hardware/Software Subscriber key generation	
6.1.9		Key usage purposes (as per X.509 v3 key usage field)	
6.2.1		Standards for cryptographic module	
6.2.4.2		Backup of subscriber private signature key	
6.4.1		Activation data generation and installation	

4.0 DETAILED ASSESSMENT

This section of the report presents the mapping comparison results for the FBCA CP and the XXXX for Rudimentary Level of Assurance requirements. This mapping comparison report works in conjunction with the FPKIPA/CPWG General Requirements CP Mapping Matrix report [4], **dated DD MM YYYY**. Following are the specific Rudimentary Level CP requirements for mapping to the FBCA CP. The mapping comparison is characterized using the evaluation terms listed in the BRIEF ASSESSMENT.

The detailed mapping results provide the FBCA and requirements to be mapped, the XXXX and appropriate applicable policy text, the evaluation result for each requirement element addressed by the XXXX, as well as the evaluation comments. By default, the evaluation results listed in the "Overall Match" field indicates all results when multiple policy elements from the XXXX are mapped to a particular FBCA CP requirement.

Table No.	CP Section	Mapping Phrase
1	FBCA: **1.2**	The OIDs are registered under the id-infosec arc as follows: Id-fpki-certpcy-rudimentaryAssurance
	XXXX:	
	Overall Match:	Comments:
2	FBCA: **1.3.4**	The sensitivity of the information processed or protected using certificates issued by FBCA or an Entity CA will vary significantly. Rudimentary - This level provides the lowest degree of assurance concerning identity of the individual. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having higher levels of assurance are unavailable.
	XXXX:	
	Overall Match:	Comments:
3	FBCA: **2.7.1**	There is no audit requirement for CAs and RAs operating at the Rudimentary or Test levels of assurance.
	XXXX:	
	Overall Match:	Comments:
4	FBCA: **3.1.1**	…Below describes the naming requirements that apply to the rudimentary level of assurance. Rudimentary – Non-Null Subject Name, or Null Subject Name if Alternative Subject Name is populated and marked critical
	XXXX:	
	Overall Match:	Comments:
5	FBCA: **3.1.9**	…summarizes the identification requirements for the rudimentary level of assurance. Rudimentary - No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
6	FBCA: **3.1.9**	The process documentation and authentication requirements shall include: - The identity of the person performing the identification; - A signed declaration by that person that he or she verified the identity of the Subscriber as required by the applicable certificate policy which may be meet by establishing how the applicant is known to the verifier as required by this certificate policy; - A unique identifying number from the ID of the verifier and, if in-person identity proofing is done, from the ID of the applicant; - The date and time of the verification; and - A declaration of identity signed by the applicant using a handwritten signature. If in-person identity proofing is done, this shall be performed in the presence of the person performing the identity authentication.
	XXXX:	
	Overall Match:	Comments:
7	FBCA: **3.2.1**	Subscribers of Entity CAs shall identify themselves for the purpose of re-keying as required below. Rudimentary - Identity may be established through use of current signature key
	XXXX:	
	Overall Match:	Comments:
8	FBCA: **4.1.1**	For all levels of assurance, this binding may be accomplished using cryptography. If cryptography is used, it must be at least as strong as that employed in certificate issuance. For Rudimentary Assurance, no trusted delivery mechanism is required.
	XXXX:	
	Overall Match:	Comments:
9	FBCA: **4.4.3.1**	…CRL issuance requirements (Routine), and CRL issuance requirements (Loss or Compromise of Private Key). Rudimentary – Not Applicable (Routine)/ Not Applicable (Loss or Compromise of Private Key).
	XXXX:	
	Overall Match:	Comments:
10	FBCA: **4.5**	Auditing capabilities are as set forth in the table below.
	XXXX:	
	Overall Match:	Comments:
11	FBCA: **4.5.2**	Frequency of processing data Rudimentary: Only required for cause
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
12	FBCA: **4.6.1**	The following minimum data shall be recorded for archive: - Entity CA accreditation - Certificate Practice Statement - Contractual obligations - System and equipment configuration - Modifications and updates to system or configuration - Certificate requests - All certificates issued or published - Record of Entity CA re-key - All audit logs
	XXXX:	
	Overall Match:	Comments:
13	FBCA: **4.6.2**	The minimum retention period for archive records is 7 years and 6 months.
	XXXX:	
	Overall Match:	Comments:
14	FBCA: **5.2.2**	Separation of Roles Rudimentary- No stipulation
	XXXX:	
	Overall Match:	Comments:
15	FBCA: **5.2.4**	At all assurance levels other than Rudimentary, an individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.
	XXXX:	
	Overall Match:	Comments:
16	FBCA: **6.1.1**	Cryptographic keying material for certificates issued by the FBCA or Entity CAs shall be generated in FIPS 140 Level 1 validated cryptographic modules.
	XXXX:	
	Overall Match:	Comments:
17	FBCA: **6.1.8**	For subscribers, software or hardware shall be used to generate pseudo-random numbers, key pairs, and symmetric keys.
	XXXX:	
	Overall Match:	Comments:
18	FBCA: **6.1.9**	Entities are encouraged at all levels of assurance to issue Subscribers two key pairs, one for data encryption and one for digital signature and authentication.
	XXXX:	
	Overall Match:	Comments:

Table No.	CP Section	Mapping Phrase
19	FBCA: **6.2.1**	… minimum requirements for XXXX cryptographic modules Rudimentary – Latest version of FIPS 140 series – N/A FBCA - Level 3 (Hardware) Certification Authority - Level 1 (Hardware or Software) Subscriber – N/A Registration Authority - Level 1 (Hardware or Software)
	XXXX:	
	Overall Match:	Comments:
20	FBCA: **6.2.4.2**	Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the FBCA rudimentary assurance policies (or an entity policy which maps to these policies) may be backed up or copied, but must be held in the Subscriber's control.
	XXXX:	
	Overall Match:	Comments:
21	FBCA: **6.4.1**	The activation data used to unlock FBCA, Entity CA or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. Rudimentary: For Rudimentary, Basic, and Medium assurance levels, activation data may be user selected.
	XXXX:	
	Overall Match:	Comments:

(Note: this information is derived from the Certificate Issuing and Management Components Protection Profile being developed by NIST.):

	Auditable Event	XXXX Rudimentary	FBCA Rudimentary
	SECURITY AUDIT		
1	Any changes to the Audit parameters, e.g., audit frequency, type of event audited		
2	Any attempt to delete or modify the Audit logs		
	IDENTIFICATION AND AUTHENTICATION		
3	Successful and unsuccessful attempts to assume a role		
4	Change in the value of maximum authentication attempts		
5	Maximum number of unsuccessful authentication attempts during user login		
6	An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		
7	An Administrator changes the type of authenticator, e.g., from password to biometrics		
	KEY GENERATION		
8	Whenever the FBCA or Entity CA generates a key. (Not		**X**

	Auditable Event	XXXX Rudimentary	FBCA Rudimentary
	mandatory for single session or one-time use symmetric keys)		
	PRIVATE KEY LOAD AND STORAGE		
9	The loading of Component private keys		**X**
10	All access to certificate subject private keys retained within the FBCA or Entity CA for key recovery purposes		**X**
	TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE		
11	All changes to the trusted public keys, including additions and deletions		**X**
	PRIVATE KEY EXPORT		
12	The export of private keys (keys used for a single session or message are excluded)		**X**
	CERTIFICATE REGISTRATION		
13	All certificate requests		**X**
	CERTIFICATE REVOCATION		
14	All certificate revocation requests		
	CERTIFICATE STATUS CHANGE APPROVAL		
15	The approval or rejection of a certificate status change request		
	FBCA OR ENTITY CA CONFIGURATION		
16	Any security-relevant changes to the configuration of the FBCA or Entity CA		
	ACCOUNT ADMINISTRATION		
17	Roles and users are added or deleted		**X**
18	The access control privileges of a user account or a role are modified		**X**
	CERTIFICATE PROFILE MANAGEMENT		
19	All changes to the certificate profile		**X**
	REVOCATION PROFILE MANAGEMENT		
20	All changes to the revocation profile		
	CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT		
21	All changes to the certificate revocation list profile		**X**
	MISCELLANEOUS		
22	*Installation of the Operating System*		
23	*Installation of the FBCA or Entity CA*		
24	*Installing hardware cryptographic modules*		
25	*Removing hardware cryptographic modules*		
26	*Destruction of cryptographic modules*		
27	*System Startup*		
28	*Logon Attempts to FBCA or Entity CA Apps*		
29	*Receipt of Hardware / Software*		
30	*Attempts to set passwords*		
31	*Attempts to modify passwords*		
32	*Backing up FBCA or Entity CA internal database*		
33	*Restoring FBCA or Entity CA internal database*		
34	*File manipulation (e.g., creation, renaming, moving)*		
35	*Posting of any material to a repository*		
36	*Access to FBCA or Entity CA internal database*		
37	*All certificate compromise notification requests*		
38	*Loading tokens with certificates*		
39	*Shipment of Tokens*		

	Auditable Event	XXXX Rudimentary	FBCA Rudimentary
40	*Zeroizing tokens*		
41	*Rekey of the FBCA or Entity CA*		**X**
	Configuration changes to the CA server involving:		
42	*Hardware*		
43	*Software*		
44	*Operating System*		
45	*Patches*		
46	*Security Profiles*		
	PHYSICAL ACCESS / SITE SECURITY		
47	*Personnel Access to room housing FBCA or Entity CA*		
48	*Access to the FBCA or Entity CA server*		
49	*Known or suspected violations of physical security*		
	ANOMALIES		
50	*Software Error conditions*		
51	*Software check integrity failures*		
52	*Receipt of improper messages*		
53	*Misrouted messages*		
54	*Network attacks (suspected or confirmed)*		
55	*Equipment failure*		
56	*Electrical power outages*		
57	*Uninterruptible Power Supply (UPS) failure*		
58	*Obvious and significant network service or access failures*		
59	*Violations of Certificate Policy*		**X**
60	*Violations of Certification Practice Statement*		**X**
61	*Resetting Operating System clock*		**X**

5.0 REFERENCES

[1] Request for Comments (RFC): 2527; Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, March 1999, http://www.ietf.org/rfc/rfc2527.txt

[2] X.509 Certificate Policy for **XXXX** Public Key Infrastructure (PKI), Revision XXXX, **DD MM YYYY**.

[3] X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), 10 September 2002.

[4] CPWG General CP Requirements Mapping for the **XXXX** PKI, **DD MM YYYY**

6.0 CONTACT DETAILS

Comments about this document may be sent to the following people:

Tim Polk, NIST 301.975.3348 tim.polk@nist.gov
Brian Dilley, Booz Allen Hamilton 410.684.6202 dilley_brian@bah.com